UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,586	06/19/2006	Benjamin Morin	33901-200PUS	1443

27799 7590 05/07/2008
COHEN, PONTANI, LIEBERMAN & PAVANE
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/583,586	MORIN ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/19/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 have been amended.

2. Claims 12-13 have been added.

3. Claims 1-13 are pending for consideration.

Priority

4. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Objections

5. Claim 4 is objected to because of the following informalities:

Regarding claim 4, the limitation "supplying alert identifiers satisfying the request and whose description cannot be refined with respect to said request" has repeated twice in this claim. Examiner interprets claim 4 as "wherein the alert management system (13) further responds to the request by supplying alert identifiers satisfying the request and whose description cannot be refined with respect to said request.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claims 1 and 12 recite the limitations "valued attributes" in line 6 and "the plurality of attribute domains" in line 8-9. There is insufficient antecedent basis for these limitations in these claims.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 11 is interpreted as being purely software per se because it comprises merely software for manipulating data.

Data structure not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. Such claimed data structures do not define any structural and functional interrelationship between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationship between the data

structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

12. Claims 1-13 are rejected under 35 U.S.C. 102(a) as being anticipated by Julisch ("Clustering Intrusion Detection Alarms to Support Root Cause Analysis"), hereinafter Julisch.

Regarding claim 1, Julisch discloses a method of managing alerts (Julisch: pages 467-468) issued by intrusion detection sensors (11a, 11b, 11c) of an information security system (1) including an alert management system (13), each alert being defined by an alert identifier and an alert content, which method includes the following steps: associating with each of the alerts issued by the intrusion detection sensors (11a, 11b, 11c) a description including a conjunction of valued attributes belonging to attribute domains (Julisch: page 449, paragraph 2, "where {A1,..., An} is the set of alarm attributes ... alarm attributes capture intrinsic alarm properties, such as the source IP address or an alarm, its destination IP address, its alarm type (which encodes the observed attack), and it time-stamp"); organizing the valued attributes belonging to each attribute domain

into a taxonomic structure defining generalization relationships between said valued attributes, the plurality of attribute domains thus forming a plurality of taxonomic structures (Julisch: page 449, paragraphs 2-4, "dom(Ai) is the domain (i.e., the range of possible value) of attribute Ai" and "generalization hierarchies"); completing the description of each of said alerts with sets of values induced by the taxonomic structures on the basis of the valued attributes of said alerts to form complete alerts (Julisch: page 449, paragraphs 2-4, "generalized alarm"); and storing said complete alerts in a logic file system (21) to enable them to be consulted (Julisch: page 450, section 4 [ALARM-CLUSTERING PROBLEMS] and pages 456-457, section 5.1 and 463-465, "alarm log").

Regarding claim 2, Julisch further discloses wherein complete alerts are consulted by successively interrogating and/or browsing said complete alerts so that the alert management system (13) responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request in order to enable said request to be refined (Julisch: pages 464-465 and 467-468, section 7).

Regarding claim 3, Julisch further discloses wherein the pertinent valued attributes assigned the highest priority are those that are most general, given the taxonomic structures (Julisch: page 464).

Regarding claim 4, Julisch further discloses wherein the alert management system (13) further responds to the request by supplying alert identifiers satisfying the request and whose description cannot be refined with respect to said request (Julisch: pages 464-465 and 467-468, section 7).

Regarding claim 5, Julisch further discloses wherein the alert identifier is a pair consisting of an identifier of the intrusion detection sensor (11a, 11b, 11c) that produces the alert and an alert serial number assigned by said sensor (Julisch: pages 449 and 452).

Regarding claim 6, Julisch further discloses wherein the content of each alert includes a text message supplied by the corresponding intrusion detection sensor (11a, 11b, 11c) (Julisch: pages 451-452).

Regarding claim 7, Julisch further discloses wherein each valued attribute includes an attribute identifier and an attribute value (Julisch: pages 449 and 451-452).

Regarding claim 8, Julisch further discloses wherein each attribute identifier is associated with one of the following attribute domains: attack domain, attacker identity domain, victim identity domain, and attack date domain (Julisch: pages 449 and 451-452).

Regarding claim 9, Julisch further discloses wherein the description of a given alert is completed by recovering recursively from generalization relationships of the taxonomic structures a set including the more general valued attributes not already included in the description of another alert completed previously (Julisch: pages 449 and 456, last paragraph).

Regarding claim 10, Julisch further discloses wherein the valued attributes in the taxonomic structure are organized in accordance with an acyclic directed graph (Julisch: pages 449 and 462).

Regarding claim 11, Julisch further discloses a computer program designed to execute the method according to claim 1, when it is executed by the alert management system (13) (Julisch: page 467-468).

Regarding claim 12, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 13, Julisch further discloses Information security system comprising intrusion detection sensors and an alert management system according to claim 12 (Julisch: page 467-468).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131